



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,887	04/05/2004	Do-heon Kim	Q79993	2675
23373 7590 12/07/2007 SUGHRUE MION, PLLC 2100 PENNSYLVANIA AVENUE, N.W. SUITE 800 WASHINGTON, DC 20037				
EXAMINER LINDSEY, MATTHEW S				
ART UNIT		PAPER NUMBER		
4152				
MAIL DATE		DELIVERY MODE		
12/07/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/816,887

Applicant(s)

KIM ET AL.

Examiner

Matthew S. Lindsey

Art Unit

4152

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 April 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 April 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SG/IC)
Paper No(s)/Mail Date See Continuation Sheet
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :13 September 2006, 10 August 2005, 16 May 2005, 10 September 2004, 12 August 2004.

DETAILED ACTION

1. Claims 1-26 are pending in this application.

Drawings

2. Figures 1, and 2a-2d should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. **Claims 1-8 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.**

5. As per Claims 1-8, Applicant has claimed "A network connection apparatus" made up of modules. The Claims lack the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 USC 101. They are not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-5, 7-16, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shah et al. (Pub. No: US 2003/0051009 A1), hereinafter Shah in view of Sherman et al. (Patent No: US 5,075,884), hereinafter Sherman.

8. With respect to Claim 1, Shah discloses: "A network connection apparatus (Abstract, lines 1-2; [0018], lines 1-4), comprising: a join module for connecting a second network ([0018], lines 1-4), to which the join module belongs, with a first network

in response to an inter-network connection request message transmitted from the first network ([0021], lines 1-6)" but does not disclose "setting a security level of the first network to a set security level, and controlling network command messages in response to the set security level".

However, Sherman discloses: "setting a security level of the first network to a set security level (Col. 4, lines 33-36, 60-61), and controlling network command messages in response to the set security level (Col. 4, lines 36-41)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communications of Shah with teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Therefore by combining the network communications of Shah with the security system of Sherman, one can communicate with a home network from an external node without unauthorized disclosure of information.

9. With respect to Claim 2, Shah discloses: "The apparatus as claimed in claim 1, wherein the join module comprises: a connection module for receiving the inter-network connection request message transmitted from the first network and connecting the first network with the second network ([0024], lines 1-3)", and "a transmission module for

transmitting a requested network command message requested by the first network ([0025], lines 4-8)", but does not disclose "an authentication/security module for determining whether to allow a connection of the first network that has transmitted the inter-network connection request message to the connection module, and setting and checking the security level of the first network" or "when the connection is allowed by the authentication/security module".

However, Sherman discloses: "an authentication/security module for determining whether to allow a connection of the first network that has transmitted the inter-network connection request message to the connection module (Col. 4, lines 49-52), and setting and checking the security level of the first network (Col. 4, lines 60-61)" and "when the connection is allowed by the authentication/security module (Col. 4, lines 52-55)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system of Shah with the teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Combining these references ensures that unauthorized disclosure of information is prevented.

10. With respect to Claim 3, Shah discloses: "The apparatus as claimed in claim 1, further comprising: a management module for collecting and managing information

Art Unit: 4152

about devices present in the second network ([0031], lines 1-3) by performing a discovery process for the devices ([0031], lines 7-10); and a component module for generating a component representing services of the devices present in the second network on a basis of the information about the devices collected by the management module ([0031], lines 3-7)".

11. With respect to Claim 4, Shah discloses: "The apparatus as claimed in claim 3, further comprising: a stack module for transmitting a control message to the devices present in the second network ([0033], lines 1-3); and a lookup service module for storing information about the component generated by the component module in a lookup table ([0031], lines 1-5), and searching for component information of a specific device upon a request for a service of the specific device ([0031], lines 10-15)".

12. With respect to Claim 5, Shah discloses: "The apparatus as claimed in claim 2, wherein the connection module contains connection information about the first network or the devices present in the first network ([0031], lines 1-5)".

13. With respect to Claim 7, Shah doesn't disclose: "The apparatus as claimed in claim 2, wherein the security level is applied differently depending on the first network to be connected".

However Sherman discloses: "The apparatus as claimed in claim 2, wherein the security level is applied differently depending on the first network to be connected (Col. 4, lines 60-61)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system of Shah with the teachings of Sherman to include a security system including multiple security levels. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Combining these references allows those of the appropriate security level to share information while preventing those without clearance to view the information.

14. With respect to Claim 8, Shah discloses: "The apparatus as claimed in claim 2, wherein the transmission module transmits the network command messages transmitted and received between the first network and the second network to which the join module belongs ([0032], lines 4-11)".

15. With respect to Claim 9, Shah discloses: "A method for connecting separate networks (Abstract, lines 1-5), comprising: (a) transmitting an initial inter-network connection request message to a second network by a first network ([0021], lines 1-5)", and "(c) transmitting a network command message to the second network by the first

network ([0021], lines 3-6)" but does not disclose: "(b) analyzing the initial inter-network connection request message and setting a security level of the first network to a set security level by the second network" or "(d) searching, by the second network, the set security level of the first network which has transmitted the network command message to generate a searched security level; (e) transmitting the searched security level and the network command message to the second network".

However, Sherman discloses: "(b) analyzing the initial inter-network connection request message and setting a security level of the first network to a set security level by the second network (Col. 4, lines 60-61)" and "(d) searching, by the second network, the set security level of the first network which has transmitted the network command message to generate a searched security level (Col. 4, lines 49-52, the guard means ensures correct security levels and manages communication); (e) transmitting the searched security level and the network command message to the second network (Col. 4, lines 49-52)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system of Shah with the teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Combining these references allows controlling access to the devices on a home network to an external network.

16. With respect to Claim 18, Shah discloses: "A method for connecting separate networks (Abstract, lines 1-5; [0018], lines 1-4), comprising: (a) receiving an initial inter-network connection request message from an external network ([0021], lines 1-5)", and "(c) receiving a network command message from the external network ([0021], lines 3-6)" but does not disclose: "(b) analyzing the initial inter-network connection request message and setting a security level of the external network to a set security level" or "(d) searching the set security level of the external network which has transmitted the network command message to generate a searched security level; (e) transmitting the searched security level and the network command message to another network to which the external network is connected".

However, Sherman discloses: "(b) analyzing the initial inter-network connection request message and setting a security level of the external network to a set security level (Col. 4, lines 60-61)" and "(d) searching the set security level of the external network which has transmitted the network command message to generate a searched security level (Col. 4, lines 49-52, the guard means ensures correct security levels and manages communication); (e) transmitting the searched security level and the network command message to another network to which the external network is connected (Col. 4, lines 49-52)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system of Shah with the teachings of Sherman to include a security system. Motivation to combine these references comes

from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Combining these references allows controlling access to the devices on a home network to an external network.

17. With respect to Claims 10 and 19, Shah discloses: "wherein the initial inter-network connection request message includes information about the first network that has transmitted the initial inter-network connection request message ([0004], lines 7-12, using TCP/IP includes sending data packets that contain headers with information about the source, in this case the header would contain information about the external network)".

18. With respect to Claims 11 and 20, Shah does not disclose: "wherein the security level is applied differently depending on the first network to be connected".

However Sherman discloses: "wherein the security level is applied differently depending on the first network to be connected (Col. 4, lines 60-61)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system of Shah with the teachings of Sherman to include a security system including multiple security levels. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area

server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Combining these references allows those of the appropriate security level to share information while preventing those without clearance to view the information.

19. With respect to Claims 12 and 21, Shah doesn't disclose: "wherein (b) comprises analyzing the initial inter-network connection request message and determining whether to allow a connection between the first and the second networks".

However, Sherman discloses: "wherein (b) comprises analyzing the initial inter-network connection request message and determining whether to allow a connection between the first and the second networks (Col. 4, lines 49-52)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communications of Shah with teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Therefore by combining the network communications of Shah with the security system of Sherman, one can communicate with a home network from an external node without unauthorized disclosure of information.

20. With respect to Claims 13 and 22, Shah "The method as claimed in claim 9, wherein (e) comprises transmitting a notify message to the first network ([0038], lines 4-11)".

21. With respect to Claims 14 and 23, Shah discloses: "The method as claimed in claim 9, further comprising: transmitting a response message for the network command message by the second network ([0026], lines 6-8)" but does not disclose "and checking a security level for the response message of the second network".

However, Sherman discloses: "and checking a security level for the response message of the second network (Col. 4, lines 42-49, to control the flow of information where different levels of security are present, it is inherent that the security levels are checked)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communications of Shah with teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Therefore by combining the network communications of Shah with the security system of Sherman, one can communicate with a home network from an external node without unauthorized disclosure of information.

22. With respect to Claims 15 and 24, Shah discloses: "further comprising, if the network command message is a search message for looking for a device present in the second network ([0036], lines 5-7)", and "and transmitting information about the devices ([0037], lines 5-10)", but does not disclose: "searching for devices corresponding to the searched security level of the first network".

However, Sherman discloses: "searching for devices corresponding to the searched security level of the first network (Col. 4, lines 42-49)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communications of Shah with teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Because the network communication system of Shah supports searching for devices, so an obvious search is for devices of a specific security level. By combining these references you are able to prevent unauthorized disclosure of information and allow searching for devices.

23. With respect to Claims 16 and 25, Shah discloses: "further comprising, if the network command message is a message for requesting information about a specific device present in the second network ([0026], lines 3-6), searching component

information about the specific device among component information about the devices present in the second network ([0031], lines 1-10) and transmitting the component information about the specific device ([0037], lines 5-10)".

24. Claims 6, 17, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shah and Sherman as applied to claims 1, 2, 9, and 18 above, and further in view of Zintel et al. (Patent No: US 6,725,281).

25. With respect to Claim 6, Shah and Sherman do not disclose: "The apparatus as claimed in claim 2, wherein the connection module checks periodically whether the first network transmits a transmitted network command message every predetermined period of time, and terminates the connection if the transmitted network command message is not received within the predetermined period of time".

However, Zintel discloses: "The apparatus as claimed in claim 2, wherein the connection module checks periodically whether the first network transmits a transmitted network command message every predetermined period of time (Col. 36, lines 13-14), and terminates the connection if the transmitted network command message is not received within the predetermined period of time (Col. 36, lines 13-15)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system and security protocol of Shah and Sherman with the teachings of Zintel to include terminating connection if a message is not received in a certain period of time. Motivation to combine these references

comes from Zintel, "The scenario is this: A UCP subscribes to a CD, then the UCP reboots. Meanwhile, the CD is still trying to send notifications to that UCP. If the UCP never comes back, the subscription would be leaked because the UCP never told the CD that it was going away." (Col. 36, lines 3-8). By combining the network communication and security system of Shah and Sherman with the timeout feature of Zintel, the network communications will be protected against leaked subscriptions.

26. With respect to Claims 17 and 26, Shah and Sherman do not disclose: "further comprising, if the network command message is not received from the first network within a predetermined period of time, terminating a connection between the first and the second networks".

However Zintel discloses: "further comprising, if the network command message is not received from the first network within a predetermined period of time (Col. 36, lines 13-14), terminating a connection between the first and the second networks (Col. 36, lines 13-15)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system and security protocol of Shah and Sherman with the teachings of Zintel to include terminating connection if a message is not received in a certain period of time. Motivation to combine these references comes from Zintel, "The scenario is this: A UCP subscribes to a CD, then the UCP reboots. Meanwhile, the CD is still trying to send notifications to that UCP. If the UCP never comes back, the subscription would be leaked because the UCP never told the

CD that it was going away." (Col. 36, lines 3-8). By combining the network communication and security system of Shah and Sherman with the timeout feature of Zintel, the network communications will be protected against leaked subscriptions.

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- a. Cheng (Pub. No: US 2002/0083143 A1) teaches a UpnP network not based on Internet Protocol.
- b. Hilt (Pub. No: EP 1175043 A1) teaches accessing a home network from an external network.
- c. Lawson et al. (Pub. No: WO 9709800 A2) teaches a home controller for controlling access to a home network.
- d. Frouin et al. (Patent No: US 7,123,614 B2) teaches communicating between a first and a second network.
- e. Wendorf et al. (Patent No: US 7,257,821 B2) teaches accessing an in home network through the internet.
- f. Shteyn (Patent No: US 6,618,764 B1) teaches interaction of two home networks with different software architectures.
- g. Kobayashi (Patent No: US 6,954,632 B2) teaches multiple home networks interacting through a security server.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew S. Lindsey whose telephone number is (571) 270-3811. The examiner can normally be reached on Mon-Thurs 7:30-5, Alternate Fridays 7:30-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil El-Hady can be reached on (571) 272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MSL
11/27/2007

/Nabil El-Hady/
Supervisory Patent Examiner, Art Unit 4152